IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
(Attorney Docket № 14182US02)

In the Application of:

Ed H. Frank, et al.

Serial No. 10/658,139

Filed: September 9, 2003

For: METHOD AND SYSTEM FOR PROVIDING SEAMLESS CONNECTIVITY AND COMMUNICATION IN A MULTI-BAND MULTI-PROTOCOL HYBRID WIRED/WIRELESS NETWORK

Examiner: Hieu T. Hoang

Group Art Unit: 2152

Confirmation No. 3006

Electronically filed on 02-SEP-2008

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from an Office Action dated April 3, 2008 ("Final Office Action"), in which claims 1-31 were finally rejected. The Appellant respectfully requests that the Board of Patent Appeals and Interferences ("Board") reverses the final rejection of claims 1-31 of the present application. The Appellant notes that this Appeal Brief is timely filed within the period for reply that ends on September 3, 2008.

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

Broadcom Corporation, a corporation organized under the laws of the state of California, and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 014225, Frame 0147 in the PTO Assignment Search room.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

The Appellant is unaware of any related appeals or interferences.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-31 were finally rejected. Pending claims 1-31 are the subject of this appeal.

The present application includes claims 1-31, which are pending in the present application. Claims 11-20 stand rejected under 35 U.S.C. § 101 as the claimed invention is directed to non-statutory subject matter. *See* Final Office Action at page 4. Claims 1-7, 9-17, 19-27, and 29-31 stand rejected under 35 U.S.C. § 102(e) as being

unpatentable by U.S. Patent No. 6,587,680, issued to Ala-Laurila, et al. (hereinafter, Laurila). *See id.* at page 4. Claims 8, 18, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Laurila, as applied to claims 1, 11, and 21, in view of U.S. Patent No. 6,651,105, issued to Bhagwat, et al. (hereinafter, Bhagwat). *See id.* at page 8. The Appellant identifies claims 1-31 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The Appellant has not amended any claims subsequent to the final rejection of claims 1-31 mailed on April 3, 2008.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

The invention of claim 1 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in pages 8-10, and in Figures 3-5. Aspects of the invention provide a method and system for providing seamless connectivity and communication in a multi-band multi-protocol hybrid wired/wireless network. *See* present application at page 8, lines 2-4, and Figure 5. The method may include initially authenticating an access device (e.g., 522 in FIG. 5) upon the access device initiating communication with a first access point (e.g., 510).

See id. at page 8, lines 4-5 and FIG. 5. Authentication information related to the initial authentication may be provided to a second access point and/or a third access point. *See id.* at page 8, lines 5-7 and FIG. 5. The first access point, second access point (e.g., 512) or third access point (e.g., 514) may provide service to the access device (e.g., 522) based on the initial authentication. *See id.* at page 8, lines 7-9 and FIG. 5.

Claims 2-10 are dependent upon claim 1.

The invention of claim 11 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in pages 8-10, and in Figures 3-5. Another embodiment of the invention may provide a machine-readable storage, having stored thereon, a computer program having at least one code section for providing seamless connectivity and communication in a multi-band, multi-protocol network. *See id.* at page 9, lines 1-4 and FIG. 5. The at least one code section may be executable by a machine, thereby causing the machine to perform the steps as described in the method for providing seamless connectivity and communication in a multi-band, multi-protocol network. *See id.* at page 9, lines 4-6 and FIG. 5.

Claims 12-20 are dependent upon claim 11.

The invention of claim 21 is illustratively described in the Specification of the present application in, for example, "Brief Summary of the Invention" section in pages 8-10, and in Figures 3-5. In accordance with another embodiment of the invention, a system for seamless connectivity and communication in a multi-band, multi-protocol network may be provided. *See id.* at page 9, lines 7-9 and FIG. 5. The system may

include at least one processor (e.g., 506a or 510a in FIG. 5) adapted to initially authenticate an access device (e.g., 522) upon the access device initiating communication with a first access point (e.g., 510). *See id.* at page 9, lines 9-11 and FIG. 5. The at least one processor may provide initial authentication information related to the initial authentication to a second access point (e.g., 512) and/or a third access point (e.g., 514). *See id.* at page 9, lines 11-13 and FIG. 5. The first access point, second access point or third access point may provide service to the access device based on the initial authentication information. *See id.* at page 9, lines 13-14 and FIG. 5.

Claims 22-31 are dependent upon claim 21.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

Claims 11-20 stand rejected under 35 U.S.C. § 101 as the claimed invention is directed to non-statutory subject matter. Claims 1-7, 9-17, 19-27, and 29-31 stand rejected under 35 U.S.C. § 102(e) as being unpatentable by U.S. Patent No. 6,587,680, issued to Ala-Laurila, et al. (hereinafter, Laurila). Claims 8, 18, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Laurila, as applied to claims 1, 11, and 21, in view of U.S. Patent No. 6,651,105, issued to Bhagwat, et al. (hereinafter, Bhagwat).

ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

In the Final Office Action, Claims 11-20 stand rejected under 35 U.S.C. § 101 as the claimed invention is directed to non-statutory subject matter. Claims 1-7, 9-17, 19-27, and 29-31 stand rejected under 35 U.S.C. § 102(e) as being unpatentable by U.S. Patent No. 6,587,680, issued to Ala-Laurila, et al. (hereinafter, Laurila). Claims 8, 18, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Laurila, as applied to claims 1, 11, and 21, in view of U.S. Patent No. 6,651,105, issued to Bhagwat, et al. (hereinafter, Bhagwat).

I. REJECTION OF CLAIMS 11-20 UNDER 35 U.S.C. § 101

The Appellant first turns to the rejection of claims 11-20 under 35 U.S.C. § 101 as being non-statutory because the claimed invention is allegedly directed to non-statutory subject matter. The Final Office Action states the following:

> "A computer-readable media, having stored thereon, a computer program," can be any transmission media (cable, wire, wireless media), signals or signal-carrying waves, and is therefore non-statutory."

See the Final Office Action at page 4. The Examiner is referred to p. 52 of the "Interim Guideline for Examination of Patent Applications for Patent Subject Matter Eligibility" (IGPSME), which states the following:

> **Data structures not claimed as embodied in computer-readable media** are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer... Similarly, **computer programs claimed as computer listings per se**, i.e., the descriptions or expressions of the programs, are not physical "things."

> They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized.

See the IGPSME at pages 52-53. Even though data structures not claimed as embodied in computer-readable media, as well as computer programs claimed as computer listings per se, are not statutory subject matter, the Appellant points out that **claims 11-20 of the present invention do not fall under any of the above mentioned non-statutory subject matter categories**. The Examiner is furthermore referred to the following IGPSME citation:

> In contrast, **a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships** between the computer program and the rest of the computer which permit the computer program's functionality to be realized, **and is thus statutory**. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.
>
> Computer programs are often recited as part of a claim. **USPTO personnel should determine whether the computer program is being claimed as part of an otherwise statutory manufacture or machine.** In such a case, **the claim remains statutory irrespective of the fact that a computer program is included in the claim. The same result occurs when a computer program is used in a computerized process where the computer executes the instructions set forth in the computer program.** Only when the claimed invention taken as a whole is directed to a mere program listing, i.e., to only its description or expression, is it descriptive material per se and hence nonstatutory.

See the IGPSME at page 53. Claims 11-20 in the present invention relate to **machine-readable storage for storing a computer program having at least one code section** for providing seamless connectivity and communication in a multi-band multi-protocol hybrid wired/wireless network. Furthermore, **the code sections may be executed by**

a machine for causing the machine to perform the method steps recited by, for example, claims 1-10. Therefore, claims 11-20 define statutory subject matter as per the above IGPSME citation.

The Examiner is also referred to the following MPEP citation for support:

> **When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and *will be statutory*** in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)

See MPEP § 2106.01. The Appellant, therefore, submits that claims 11-20 are directed to statutory subject matter, and that the rejection of claims 11-20 under 35 USC § 101 should be withdrawn.

As additional comment, the Appellant points out that numerous issued patents use "machine-readable" type claims as part of their allowed claims. In fact, at least six patents were issued on 8/26/2008 alone, using "machine-readable" type claims (the Examiner is referred to US patents 7418625, 7418568, 7418560, 7418304, 7417986, and 7417569).

II. REJECTION UNDER 35 U.S.C. § 102

With regard to the anticipation rejections under 102, MPEP 2131 states that:

> "[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *See* Manual of Patent Examining Procedure (MPEP) at 2131 (internal citation omitted) (emphasis added). Furthermore, "[t]he

identical invention must be shown in as complete detail as is contained in the ... claim." *See* id. (internal citation omitted).

A. Rejection of Independent Claims 1, 11 and 21

With regard to the rejection of independent claim 1 under 102(e), The Appellant submits that Laurila does not disclose or suggest at least the limitation of "providing authentication information related to said initial authentication to at least one of a second access point and a third access point," as recited in claim 1 by the Appellant.

The Examiner states the following in the Final Office Action regarding Laurila:

"Laurila discloses a method for providing seamless connectivity and communication in a multi-band, multi-protocol network (abstract), the method comprising:

initially authenticating an access device upon said access device initiating communication with a first access point (fig. 3, col 8 lines 62-67, AP_old or the old access point that mobile terminal 12 is originally communicating and about to disconnect to hand-over to a new access point, or AP_new 114; SA or security association, read as authentication information, is retrieved from AP_old, suggesting that AP_old has stored authentication information of mobile terminal 12 for the original communication);

providing authentication information related to said initial authentication to at least one of a second access point and a third access point (fig. 3, HO_request, a handover request containing authentication information is sent from AP_old to AP_new); and

servicing said access device by one of said first access point, said second access point and said third access point based on said initial authentication (fig. 3, payload traffic or servicing can be resumed between the mobile terminal and the new AP)."

See the Final Office Action at page 4. The Examiner seems to equate Laurila's disclosure of the security association (SA) to the Appellant's "initial authentication," as

recited in claim 1. The Appellant respectfully disagrees and points out that Laurila's "security function" and "authentication" are two separate and distinct functions. For example, as explained herein below, Laurila's mobile terminal MT 12 (asserted as an access device by the Examiner) and the new access point AP_new 114 are each separately and independently authenticated through a procedure of generating challenges and comparing the calculated response with the correct response. There is no Security Association (SA) parameter involved in the authentication procedure. In other words, **Laurila's SA parameter exchange procedure is separate and independent of the authentication procedure using challenges and responses**.

The Examiner is referred to the following Laurila citation regarding the security association (SA):

> "...a security association (SA) exists between mobile terminal 12 and the current or old-AP 14. That is, it will be assumed that mobile terminal 12 and AP 14 share the same common 5 set of keys and other information that is necessary **to achieve the security function(s)**."

See Laurila at col. 8 lines 2-6. The Appellant points out that Laurila clearly discloses that the SA utilizes a common set of keys, which are necessary to achieve security function(s). The Examiner is further referred to the following Laurila citation:

> "In accordance with the invention, this established and shared **security association is transferred from old-AP 14 to new-AP 114, in a secure fashion**, as mobile terminal moves from cell 18 to cell 118. This transfer 1o is made in a very fast manner by **minimizing the number of message that are needed** to effect the transfer, and by **eliminating the use of public key encryption**. As a result, **the interruption of a payload traffic transfer to and from mobile terminal 12 is minimized**, any interruption

> of this type being very important for real-time services such as Voice over IP (VOIP) and video distribution."

See Laurila at col. 8 lines 6-16. Instead of using SA for authentication procedure in the mobile terminal MT 12 and in the AP_new 114, as asserted by the Examiner, Laurila discloses that **the transfer of SA is for purposes of eliminating the use of public key encryption (for security) and for minimizing the additional messages needed (message encryption and decryption).** Laurila clearly discloses the benefits of transferring SA, namely, to minimize delays in services such as VOIP and video distribution. **In other words, Laurila discloses that the SA parameter is retrieved and transferred for the purpose of minimizing the need of exchanging security messages that would otherwise cause undesirable delays in certain types of services. There is no disclosure or suggestion by Laurila that the SA is utilized as information to facilitate authentication in the MT 12 and the AP_new 114.**

Therefore, the Appellant maintains that Laurila does not disclose or suggest that "the SA is stored and read as authentication information, retrieved from AP_old," as asserted by the Examiner.

The Examiner is further referred to the following citations in Laurila regarding the authentication procedure, where the generation of challenges and calculating of responses between the MT 12 and the AP_new 114 are separated from the SA. Specifically, Laurila discloses the following:

> "Later, when **mobile terminal 12 moves from cell 18 and its AP 14 to cell 118 and its AP 114, authentication during the handover process** is achieved by the invention's simple **challenge/response procedure**...

> During the challenge/response procedure, new-AP 118 sends a challenge to mobile terminal 12, whereupon mobile terminal 12 sends a response to new-AP 118. In addition, **mobile terminal 12 authenticates new-AP 118** in a similar manner during the handover."

See Laurila at col. 8 lines 23-34. Laurila discloses that new authentication is required for the mobile terminal 12 moving from cell 18 (form AP_old 14, asserted as the first access point by the Examiner) to the new cell 118 (to AP_new 114, asserted as the second access point by the Examiner) through a series of challenge and response procedure (ap_response, mt_response and ap_challenge, mt_challenge), which are separate and unrelated to the SA parameters.

For example, Fig. 2 of Laurila describes a forward handover process 20 as follows:

> "FIG. 2 shows a forward handover (HO) process 20 in accordance with the invention, ... In forward handover process 20 the handover signaling is sent between mobile terminal (MT or mt) 12 and new-access point (AP or ap) 114. This type of handover is especially useful when radio link 21 is lost without prior warning."

See Laurila at col. 8 lines 42-48. Laurila discloses that the mobile terminal MT 12 generates a challenge (mt_challenge) and is sent as a message MAC_REASSOCIATE_REQ to the AP_new 114. The AP_new 114 sends back a reply message MAC_AUTHENTICATE_REQ with a generated challenge (ap_challenge) and a calculated response (ap_response). The MT 12 performs an authentication (AP Authentication) by comparing the ap_response with the correct response. The MT 12 replies with a message MAC_AUTHENTICATE_RESP carrying a response (mt_response) to the AP_new 114. The AP_new 114 performs an authentication (MT

Authentication) by comparing the mt_response to the correct response. Upon successful authentication, the AP_new 114 returns a message MAC_REASSOCIATE_RESP to confirm successful handover so that the payload traffic can be resumed (see Laurial in Fig. 2). **The Appellant points out that no SA information is used in any of the authentication messages throughout the entire authentication process.**

Similarly, the Examiner is referred to Fig. 3 of Laurila, describing a backward handover process 30 as follows:

> "FIG. 3 shows a backward handover (HO) process 30 in accordance with the invention. In backward handover process 30 handover is requested by mobile terminal 12 communication with old-AP 14 ... During a backward handover a beneficial option is to use the radio interface message 31 that carries the authentication challenge from old-AP 14 to mobile terminal 12 to also trigger backward handover 33. That is, authentication challenge 31 is used to indicate to mobile terminal 12 that it should disconnect from old-AP 14 and connect to new-AP 114 whereat a security association (SA) 35 has already been prepared for mobile terminal 12."

See Laurila at col. 10, lines 53-61. Laurila in Fig. 3 discloses that the AP_new 114 receives a handover request HO_REQUEST from the AP_old 14. The AP_new 114 generates a challenge (ap_challenge) and sent as a message HO_RESPONSE 35 to the first access point AP_old 14. The AP_old 14 forwards the same ap_challenge in a message MAC_DISASSOCIATE 31 to the MT 12 to trigger a backward handover process. The mobile terminal MT 12 replies to the AP_new 114 with a message MAC_REASSOCIATE_REQ (mt_response, mt_challenge, other info). The AP_new 114 authenticates the mobile terminal 12 by comparing to the mt_response with a

correct response. A new response ap_response is calculated based on the mt_challenge and is sent back to the mobile terminal MT 12 as a message MAC_REASSOCIATE_RESP_ENH (ap_respoonse). The MT 12, authenticates the AP_new 114 by comparing to the ap_respoonse with a correct response. A successful authentication procedure in both the AP_new and mobile terminal 12 confirms the backward handover and the payload traffic can be resumed. **The Appellant again points out that no SA information is used in any of the authentication messages throughout the entire authentication process.**

To summarize the above arguments, Laurila discloses that the SA parameters are for security information sharing during connection process when the MT 12 is moved from an AP_old 14 to an AP_new 114 to minimize interruptions caused by additional security messages. Laurila discloses that a separate authentication procedure is required in the hand over process, and the SA exchange is not related in any way to Laurila's authentication procedure.

Based on the foregoing arguments, the Appellant maintains that **the SA parameter exchange is not "initial authentication,"** as asserted by the Examiner. Therefore, Laurila does not disclose or suggest "providing authentication information related to said initial authentication to at least one of a second access point and a third access point," as recited in claim 1 by the Appellant.

With regard to the rejection of independent claim 1 under 102(e), Appellant further submits that Laurila does not disclose or suggest at least the limitation of

"servicing said access device by one of said first access point, said second access point and said third access point based on said initial authentication," as recited in claim 1 by the Appellant.

Based on the foregoing arguments that the SA is not disclosed or suggested as "initial authentication" by Laurila, and new authentications are required by both the mobile terminal MT 12 and the AP_new 114 during the handover, subsequently, the Appellant maintains that Laurila does not disclose or suggest "**servicing** said access device by one of said first access point, said second access point and said third access point **based on said initial authentication,**" as recited in claim 1 by the Appellant.

Accordingly, the Appellant respectfully submits that claim 1 is not anticipated by Laurila, and therefore is allowable. The Appellant respectfully requests that the rejection of claim 1 under 35 U.S.C. § 102(e) be withdrawn.

Independent claims 11 and 21 are similar in many respects to independent claim 1. Therefore, the Appellant respectfully submits that claims 11 and 21 are also allowable at least for the reasons stated above with regard to claim 1, and respectfully requests that the rejection of claims 1, 11 and 21 under 35 U.S.C. § 102(e) be withdrawn.

Furthermore, the Appellant reserves the right to argue additional reasons beyond those set forth herein to support the allowability of independent claims 1, 11 and 21, should such a need arise.

B. Rejection of Dependent Claims 2, 12, and 22

Claims 2, 12, and 22 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 2, 12, and 22 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "storing said initial authentication information," as recited by the Appellant in claims 2, 12, and 22.

With regard to claims 2, 12, and 22, the Final Office Action states the following at page 5:

> For claims 2, 12, and 22, Laurila further discloses storing said initial authentication information (fig. 3, AP_old has stored the authentication information of terminal 12 for the original communication).

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient since AP_old does not store any of the SA. Laurila only discloses that AP_old 14 only **retrieves** the SA parameters from the SA database. Laurila clearly does not disclose or suggest "storing said initial authentication information," as recited by the Appellant in claims 2, 12, and 22. Accordingly, the Appellant submits that claims 2, 12, and 22 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2, 12, and 22.

C. Rejection of Dependent Claims 3, 13, and 23

Claims 3, 13, and 23 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 3, 13, and 23 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "retrieving said stored initial authentication information by said second access point and said third access point," as recited by the Appellant in claims 3, 13, and 23.

With regard to claims 3, 13, and 23, the Final Office Action states the following at page 6:

> For claims 3, 13, and 23, Laurila further discloses retrieving said stored initial authentication information by said second access point and said third access point (fig. 3, HO_request, a handover request containing authentication information of device 12 is sent from AP_old to AP_new).

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Even if authentication information (SA) is sent from AP_old to AP_new, **Laurila still does not disclose that authentication information is retrieved by two separate access points**, as recited in Appellant's claim 3. In this regard,

Laurila clearly does not disclose or suggest "retrieving said stored initial authentication information by said second access point and said third access point," as recited by the Appellant in claims 3, 13, and 23. Accordingly, the Appellant submits that claims 3, 13, and 23 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 3, 13, and 23.

D. Rejection of Dependent Claims 4, 14, and 24

Claims 4, 14, and 24 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 4, 14, and 24 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "said retrieving comprises retrieving said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point," as recited by the Appellant in claims 4, 14, and 24.

With regard to claims 4, 14, and 24, the Final Office Action states the following at page 6:

> For claims 4, 14, and 24, Laurila further discloses said retrieving comprises retrieving said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point (fig. 3, a handover is when the mobile terminal migrates from a first coverage area of AP_old to a second coverage area of AP_new).

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Laurila discloses that the SA is only retrieved by the AP_old 14 and it is then communicated to the "second access point" (AP_new). In this regard, the SA is not retrieved by two separate access points, as recited in Appellant's claim 3. Furthermore, the SA is also not retrieved by the second access point (AP_new) since the SA has already been retrieved by AP_old and then communicated to AP_new. Laurila clearly does not disclose or suggest "said retrieving comprises retrieving said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point," as recited by the Appellant in claims 4, 14, and 24. Accordingly, the Appellant submits that claims 4, 14, and 24 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 4, 14, and 24.

E. Rejection of Dependent Claims 5, 15, and 25

Claims 5, 15, and 25 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 5, 15, and 25 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "retrieving said initial authentication information by said third access point when said access device migrates from one of said first coverage area and said second coverage area to a third coverage area associated with said third access point," as recited by the Appellant in claims 5, 15, and 25.

With regard to claims 5, 15, and 25, the Final Office Action states the following at page 6:

> For claims 5, 15, and 25, the claims are rejected for the same rationale as in claim 4. A handover to a third access point is the same as the handover from the old access point to the new access point.

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Laurila discloses that the SA is only retrieved by the AP_old 14 and it is then communicated to the "second access point" (AP_new). In this regard, the SA is not retrieved by two separate access points, as recited in Appellant's claim 3. Furthermore, Laurila does not disclose that the SA is also retrieved by a third access

point (AP_new is already equated as a "second access point"). Even if another access point is considered as the "third access point", the fact remains that the SA has already been retrieved by AP_old and then communicated to AP_new or the third access point, i.e., only AP_old performs the retrieving. Laurila clearly does not disclose or suggest "retrieving said initial authentication information by said third access point when said access device migrates from one of said first coverage area and said second coverage area to a third coverage area associated with said third access point," as recited by the Appellant in claims 5, 15, and 25. Accordingly, the Appellant submits that claims 5, 15, and 25 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 5, 15, and 25.

F. Rejection of Dependent Claims 6, 16, and 26

Claims 6, 16, and 26 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 6, 16, and 26 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "retrieving said initial authentication information upon said access device initiating communication with said second access point," as recited by the Appellant in claims 6, 16, and 26.

With regard to claims 6, 16, and 26, the Final Office Action states the following at pages 6-7:

> For claims 6, 16, and 26, Laurila further discloses said retrieving comprises retrieving said initial authentication information upon said access device initiating communication with said second access point (fig. 2, radio handover, HO_request, HO_response(SA,SA), the new access point retrieves the initial authentication information of the mobile terminal previously stored at the old access point upon the device initiating communication with the new access point).

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Laurila discloses that the SA is only retrieved by the AP_old 14 and it is then communicated to the "second access point" (AP_new). In this regard, the SA is not retrieved by two separate access points, as recited in Appellant's claim 3. Furthermore, the SA is also not retrieved by the new (second) access point (AP_new) since the SA has already been retrieved by AP_old and then communicated to AP_new. Laurila clearly does not disclose or suggest "retrieving said initial authentication information upon said access device initiating communication with said second access point," as recited by the Appellant in claims 6, 16, and 26. Accordingly, the Appellant submits that claims 6, 16, and 26 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 6, 16, and 26.

G. Rejection of Dependent Claims 7, 17, and 27

Claims 7, 17, and 27 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 7, 17, and 27 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "retrieving said initial authentication information upon said access device initiating communication with said third access point," as recited by the Appellant in claims 7, 17, and 27.

With regard to claims 7, 17, and 27, the Final Office Action states the following at page 7:

> For claims 7, 17, and 27, the claims are rejected for the same rationale as in claim 6.

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Laurila discloses that the SA is only retrieved by the AP_old 14 and it is then communicated to the "second access point" (AP_new). In this regard, the SA is not retrieved by two separate access points, as recited in Appellant's claim 3. Furthermore, Laurila does not disclose that the SA is also retrieved by a third access point (AP_new is already equated as a "second access point"). Even if another access point is considered as the "third access point", the fact remains that the SA has already

been retrieved by AP_old and then communicated to AP_new or the third access point, i.e., only AP_old performs the retrieving. Laurila clearly does not disclose or suggest "retrieving said initial authentication information upon said access device initiating communication with said third access point," as recited by the Appellant in claims 7, 17, and 27. Accordingly, the Appellant submits that claims 7, 17, and 27 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 7, 17, and 27.

H. Rejection of Dependent Claims 9, 19, and 29

Claims 9, 19, and 29 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 9, 19, and 29 are allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "transparently transferring said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point," as recited by the Appellant in claims 9, 19, and 29.

With regard to claims 9, 19, and 29, the Final Office Action states the following at page 7:

> For claims 9, 19, and 29, Laurila further discloses transparently transferring said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point (fig. 2, HO_request, HO_response, fig. 3, HO_response, transferring authentication information from the old access point to the new access point during a handover between the two).

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Since the SA is communicated within the handover request, the Appellant submits that there is no "transparent transferring" of the SA. Therefore, Laurila does not disclose or suggest "transparently transferring said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point," as recited by the Appellant in claims 9, 19, and 29. Accordingly, the Appellant submits that claims 9, 19, and 29 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 9, 19, and 29.

I. Rejection of Dependent Claims 10, 20, and 30

Claims 10, 20, and 30 depend on independent claims 1, 11, and 21, respectively. Therefore, the Appellant submits that claims 10, 20, and 30 are allowable over the

reference cited in the Final Office Action at least for the reasons stated above with regard to claim 1. The Appellant also submits that Laurila does not disclose or suggest at least the limitation of "transparently transferring said initial authentication information to said third access point during a handoff of said access device from one of said first access point and said second access point to said third access point," as recited by the Appellant in claims 10, 20, and 30.

With regard to claims 10, 20, and 30, the Final Office Action states the following at page 7:

> For claims 10, 20, and 30, the claims are rejected for the same rationale as in claim 9.

As already explained in Section II-A above, Laurila's SA is not authentication information as it is not used for purposes of authentication. Even if we assume for the sake of argument that Laurila's SA is authentication information, the Examiner's argument is still deficient. Since the SA is communicated within the handover request, the Appellant submits that there is no "transparent transferring" of the SA. Therefore, Laurila does not disclose or suggest "transparently transferring said initial authentication information to said third access point during a handoff of said access device from one of said first access point and said second access point to said third access point," as recited by the Appellant in claims 10, 20, and 30. Accordingly, the Appellant submits that claims 10, 20, and 30 are allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 10, 20, and 30.

J. Rejection of Dependent Claim 31

Claim 31 depends on independent claim 21. Therefore, the Appellant submits that claim 31 is allowable over the reference cited in the Final Office Action at least for the reasons stated above with regard to claim 21. Accordingly, the Appellant submits that claim 31 is allowable over the reference cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 31.

III. REJECTION UNDER 35 U.S.C. § 103

A. The Proposed Combination of Laurila and Bhagwat Does Not Render Claims 8, 18, 28 Unpatentable

The Appellant turns to the rejection of claims 8, 18, and 28 under 35 U.S.C. § 103(a) as being anticipated over Laurila in view of Bhagwat.

With regard to the rejection of dependent claims 8, 18 and 28, the Examiner, at page 8 of the Final Office Action, concedes that "Laurila does not disclose distributing said initial authentication information to said second access point and said third access

point upon said initial authenticating." The Examiner looks to Bhagwat's Fig. 5 to teach the deficiencies of Laurila and states the following in the Final Office Action:

> However, Bhagwat discloses distributing said initial authentication information to said second access point and said third access point upon said initial authenticating (fig.5, authentication server, col. 7 lines 34-42, col. 10 lines 14-34, a centralized authentication server stores authentication information of mobile devices as they move from one access point to the next)...to implement a centralized authentication server for distributing authentication information in a dynamic fashion among PPP backend servers and further access points (Bhagwat, col. 10 lines 22-26).

See the Final Office Action at page 8. The Examiner uses the following Bhagwat citations:

> "...one embodiment uses a central PPP authentication database for all PPP backend servers. A PPP server consults this central server **to retrieve** the authentication information of a mobile user."

See Bhagwat at col. 10, lines 27-30. The Appellant points out that Bhagwat discloses a mobile user **retrieving** authentication information from the central PPP authentication data base in the central server. Bhagwat, however, does not disclose "**distributing** said initial authentication information to **said second access point and said third access point upon said initial authenticating**," The Appellant has further reviewed the citations in Bhagwat (fig.5, authentication server, col 7 lines 34-42, col. 10 lines 14-34) and cannot find support to the assertion made by the Examiner on the disclosure of the claimed limitation of "**distributing** said initial authentication information to **said second access point and said third access point upon said initial authenticating**," as recited in claims 8, 18 and 28 by the Appellant. Therefore, the Appellant submits that claims 8, 18 and 28 are also allowable.

Moreover, dependent claims 8, 18 and 28 depend from independent claims 1, 11 and 21, respectively. Consequently, claims 8, 18 and 28 are also respectfully submitted to be allowable at least for the reasons stated above with regard to claim 1. The Appellant respectfully requests that the rejection of claims 8, 18 and 28 under 35 U.S.C. § 103(a) be withdrawn.

Furthermore, the Appellant reserves the right to argue additional reasons beyond those set forth herein to support the allowability of dependent claims 8, 18 and 28, should such a need arise.

CONCLUSION

For at least the foregoing reasons, the Appellant submits that claims 1-31 are in condition for allowance. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge $510 (to cover the Brief on Appeal Fee) and any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: 02-SEP-2008

By: /Ognyan I. Beremski/
Ognyan Beremski, Reg. No. 51,458
Attorney for Appellant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775 – 8100

(OIB)

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method for providing seamless connectivity and communication in a multi-band, multi-protocol network, the method comprising:

initially authenticating an access device upon said access device initiating communication with a first access point;

providing authentication information related to said initial authentication to at least one of a second access point and a third access point; and

servicing said access device by one of said first access point, said second access point and said third access point based on said initial authentication.

2. The method according to claim 1, comprising storing said initial authentication information.

3. The method according to claim 2, comprising retrieving said stored initial authentication information by said second access point and said third access point.

4. The method according to claim 3, wherein said retrieving comprises retrieving said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point.

5. The method according to claim 4, wherein said retrieving comprises retrieving said initial authentication information by said third access point when said access device migrates from one of said first coverage area and said second coverage area to a third coverage area associated with said third access point.

6. The method according to claim 3, wherein said retrieving comprises retrieving said initial authentication information upon said access device initiating communication with said second access point.

7. The method according to claim 3, wherein said retrieving comprises retrieving said initial authentication information upon said access device initiating communication with said third access point.

8. The method according to claim 1, comprising distributing said initial authentication information to said second access point and said third access point upon said initial authenticating.

9. The method according to claim 5, comprising transparently transferring said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point.

10. The method according to claim 5, comprising transparently transferring said initial authentication information to said third access point during a handoff of said access device from one of said first access point and said second access point to said third access point.

11. A computer-readable media, having stored thereon, a computer program having at least one code section for providing seamless connectivity and communication in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

initially authenticating an access device upon said access device initiating communication with a first access point;

providing authentication information related to said initial authentication to at least one of a second access point and a third access point; and

servicing said access device by one of said first access point, said second access point and said third access point based on said initial authentication.

12. The computer-readable media according to claim 11, wherein said at least one code section comprises code for storing said initial authentication information.

13. The computer-readable media according to claim 12, wherein said at least one code section comprises code for retrieving said stored initial authentication information by said second access point and said third access point.

14. The computer-readable media according to claim 13, wherein said at least one code section comprises code for retrieving said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point.

15. The computer-readable media according to claim 14, wherein said at least one code section comprises code for retrieving said initial authentication information by said third access point when said access device migrates from one of said first coverage area and said second coverage area to a third coverage area associated with said third access point.

16. The computer-readable media according to claim 13, wherein said at least one code section comprises code for retrieving said initial authentication information upon said access device initiating communication with said second access point.

17. The computer-readable media according to claim 13, wherein said at least one code section comprises code for retrieving said initial authentication information upon said access device initiating communication with said third access point.

18. The computer-readable media according to claim 11, wherein said at least one code section comprises code for distributing said initial authentication information to said second access point and said third access point upon said initial authenticating.

19. The computer-readable media according to claim 15, wherein said at least one code section comprises code for transparently transferring said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point.

20. The computer-readable media according to claim 15, wherein said at least one code section comprises code for transparently transferring said initial authentication information to said third access point during a handoff of said access device from one of said first access point and said second access point to said third access point.

21. A system for providing seamless connectivity and communication in a multi-band, multi-protocol network, the system comprising:

at least one processor for initially authenticating an access device upon said access device initiating communication with a first access point;

said at least one processor for providing authentication information related to said initial authentication to at least one of a second access point and a third access point; and

said one of said first access point, said second access point and said third access point providing service to said access device based on said initial authentication..

22. The system according to claim 21, comprising at least one memory for storing said initial authentication information.

23. The system according to claim 22, wherein said at least one processor retrieves said stored initial authentication information by said second access point and said third access point.

24. The system according to claim 23, wherein said at least one processor retrieves said initial authentication information by said second access point when said access device migrates from a first coverage area associated with said first access point to a second coverage area associated with said second access point.

25. The system according to claim 24, wherein said at least one processor retrieves said initial authentication information by said third access point when said

access device migrates from one of said first coverage area and said second coverage area to a third coverage area associated with said third access point.

26. The system according to claim 23, wherein said at least one processor retrieves said initial authentication information upon said access device initiating communication with said second access point.

27. The system according to claim 23, wherein said at least one processor retrieves said initial authentication information upon said access device initiating communication with said third access point.

28. The system according to claim 21, wherein said at least one processor distributes said initial authentication information to said second access point and said third access point upon said initial authenticating.

29. The system according to claim 25, wherein said at least one processor transparently transfers said initial authentication information to said second access point during a handoff of said access device from said first access point to said second access point.

30. The system according to claim 25, wherein said at least one processor transfers said initial authentication information to said third access point during a

handoff of said access device from one of said first access point and said second access point to said third access point.

31. The system according to claim 25, wherein said at least one processor is an authentication processor, a switch processor, an access point processor and a server processor.

EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

(1) United States Patent No. 6,587,680 ("Laurila"), entered into record by the Examiner in the May 2, 2007 Office Action.

(2) United States Patent No. 6,651,105 ("Bhagwat"), entered into record by the Examiner in the May 2, 2007 Office Action.

RELATED PROCEEDINGS APPENDIX
(37 C.F.R. § 41.37(c)(1)(x))

The Appellant is unaware of any related appeals or interferences.